

ÍNDICE

- 1.Adquisición de memoria ram
- 2.Volatility
- 2.1 Windows.pslist.PsList
- 2.2 Windows.psscan.PsScan
- 2.3 Windows.pstree.PsTree
- 2.4 Windows.privileges.Privs

1. Adquisición de memoria ram

```
:\Herramientas>winpmem_mini_x64_rc2.exe windows_ram.mem
WinPmem64
Extracting driver to C:\Users\forensic\AppData\Local\Temp\pmeBEB1.tmp
Driver Unloaded.
Loaded Driver C:\Users\forensic\AppData\Local\Temp\pmeBEB1.tmp.
Deleting C:\Users\forensic\AppData\Local\Temp\pmeBEB1.tmp
The system time is: 19:25:35
Will generate a RAW image
- buffer_size_: 0x1000
CR3: 0x00001A0000
CR3: 0x00001AA000
CR3: 0x00001AA000

4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x001000000 - Length 0x00002000
Start 0x00103000 - Length 0xDFEED000
Start 0x100000000 - Length 0x5F300000
max_physical_memory_ 0x15f300000
Acquitision mode PTE Remapping
Padding from 0x000000000 to 0x00001000
  - length: 0x1000
 opy_memory
- start: 0x1000
 - end: 0x9f000
00% 0x00001000 .
Padding from 0x0009F000 to 0x00100000
 - length: 0x61000
00% 0x0009F000 .
copy_memory
- start: 0x100000
 - end: 0x102000
00% 0x00100000 .
Padding from 0x00102000 to 0x00103000
 - length: 0x1000
00% 0x00102000 .
copy_memory
- start: 0x103000
 - end: 0xdfff0000
00% 0x00103000 .....
14% 0x32103000 .........
28% 0x64103000 ....
42% 0x96103000 ......
56% 0xC8103000 .....
Padding from 0xDFFF0000 to 0x100000000
pad
 - length: 0x20010000
63% 0xDFFF0000 .....
copy_memory
 - start: 0x100000000
 - end: 0x15f300000
72% 0x100000000 ........
87% 0x1320000000 .....
The system time is: 19:29:24
Driver Unloaded.
```

La máquina a la que vamos a extraer la memoria ram es una máquina virtual cuyo sistema operativo es Windows 10.

Para la adquisición hemos utilizado la herramienta "winpmem_mini_x64_rc2.exe" con el siguiente comando:

"C:\Herramientas> winpmem_mini_x64_rc2.exe windows_ram.mem" que lo que ha hecho es guardarnos una copia de la memoria en el archivo (imagen) que hemos denominado "Windows_ram.mem"

```
C:\Users\forensic>ping google.es

Haciendo ping a google.es [142.250.184.3] con 32 bytes de datos:
Respuesta desde 142.250.184.3: bytes=32 tiempo=14ms TTL=116
Respuesta desde 142.250.184.3: bytes=32 tiempo=12ms TTL=116
Respuesta desde 142.250.184.3: bytes=32 tiempo=21ms TTL=116
Respuesta desde 142.250.184.3: bytes=32 tiempo=12ms TTL=116

Estadísticas de ping para 142.250.184.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 12ms, Máximo = 21ms, Media = 14ms
```

Cuando hemos ejecutado la herramienta "Winpmem_mini_x64_rx2.exe" hemos lanzado también un ping al dominio de "Google.es" para que lo captara también a la hora de adquirir la memoria ram.

2.Volatility

2.1 Windows.pslist.PsList

		ramework 2.4.0										
ogre D	ss: 100 PPID	.00 ImageFileName	PDB scanning fi Offset(V)		Handle	s Session	nId	Wow64	CreateTime	ExitTi	me	File ou
	0	System 0xe38ab			N/A	False			7:01.000000	N/A	Disabl	
8	4	Registry	0xe38ab1fba040	4		N/A	False		-26 18:36:34		N/A	Disable
8		smss.exe	0xe38ab3e7f040	2		N/A	False		-26 18:37:01		N/A	Disable Disable
4	448	csrss.exe	0xe38ab4f0b080	11 1		0	False		-26 18:37:22		N/A	
2	448	wininit.exe	0xe38ab4a80080	1		0 1	False False		-26 18:37:24		N/A	Disabl
	536	csrss.exe	0xe38ab4a85140						-26 18:37:24		N/A	Disabl
2	536	winlogon.exe	0xe38ab4555080	6		1	False		-26 18:37:24		N/A	Disabl
0	544	services.exe	0xe38ab4a83140	10		0	False		-26 18:37:25		N/A	Disabl
6	544	lsass.exe	0xe38ab4ca4080	12		0	False		-26 18:37:25		N/A	Disabl
14	680	svchost.exe	0xe38ab873a340	15		0	False		-26 18:37:27		N/A	Disabl
8	612	fontdrvhost.ex		5		1	False		-26 18:37:28		N/A	Disabl
6	544	fontdrvhost ex		5		0	False		-26 18:37:28		N/A	Disabl
8	680	svchost.exe	0xe38ab4c09080	18		0	False		-26 18:37:28		N/A	Disabl
0	680	svchost.exe	0xe38ab8224340	6		0	False		-26 18:37:28		N/A	Disabl
0	680	svchost.exe	0xe38ab851d340			0	False		-26 18:37:30		N/A	Disabl
32	680	svchost.exe	0xe38ab85230c0	4		0	False		-26 18:37:30		N/A	Disabl
40	680	svchost.exe	0xe38ab852b080			0	False		-26 18:37:30		N/A	Disabl
56	680	svchost.exe	0xe38ab852a080			0	False		-26 18:37:30		N/A	Disabl
80	680	svchost.exe	0xe38ab854a080	4		0	False		-26 18:37:30		N/A	Disabl
28	680	svchost.exe	0xe38ab8581080	8		0	False		-26 18:37:31		N/A	Disabl
40	680	svchost.exe	0xe38ab8584340			0	False		-26 18:37:31		N/A	Disabl
48	680	svchost.exe	0xe38ab8587340	12		0	False		-26 18:37:31		N/A	Disabl
32	680	svchost.exe	0xe38ab85b9080			0	False	2023-12	-26 18:37:31	.000000	N/A	Disabl
40	680	svchost.exe	0xe38ab85bc0c0			0	False	2023-12	-26 18:37:31	.000000	N/A	Disabl
92	680	svchost.exe	0xe38ab8621340			0	False	2023-12	-26 18:37:31	.000000	N/A	Disabl
44	680	svchost.exe	0xe38ab8627080			0	False	2023-12	-26 18:37:32	.000000	N/A	Disabl
16	680	svchost.exe	0xe38ab86780c0			0	False	2023-12	-26 18:37:33	.000000	N/A	Disabl
84	680	svchost.exe	0xe38ab1e86080			0	False	2023-12	-26 18:37:33	.000000	N/A	Disabl
88	680	svchost.exe	0xe38ab454d080	8		0	False		-26 18:37:34		N/A	Disabl
28	680	VBoxService.ex		11		0	False		-26 18:37:35		N/A	Disabl
76	680	svchost.exe	0xe38ab8a22080	2		0	False		-26 18:37:35		N/A	Disabl
20	680	svchost.exe	0xe38ab8a7d080			0	False		-26 18:37:36		N/A	Disabl
28	680	svchost.exe	0xe38ab8a7f0c0	9		0	False		-26 18:37:36		N/A	Disabl
48	680	svchost.exe	0xe38ab8a8d340	4		0	False		-26 18:37:36		N/A	Disabl
64	680	svchost.exe	0xe38ab4fe30c0	10		0	False		-26 18:37:36		N/A	Disabl
08	4	MemCompression		26		N/A	False		-26 18:37:37		N/A	Disabl
64	680	svchost.exe	0xe38ab8abf340	2		0	False		-26 18:37:37		N/A	Disabl
76	680	svchost.exe	0xe38ab8ac0080	3		0	False		-26 18:37:37		N/A	Disabl
40	680	svchost.exe	0xe38ab88720c0	6		0	False		-26 18:37:37		N/A	Disabl
48	680	svchost.exe	0xe38ab8877080	3		0	False		-26 18:37:37		N/A	Disabl
68	680	svchost.exe	0xe38ab887b0c0	2		0	False		-26 18:37:38		N/A	Disabl
16	680	svchost.exe	0xe38ab888830c0	11		0	False		-26 18:37:38 -26 18:37:38		N/A	Disabl
36	680	svchost.exe	0xe38ab88a0080	5		0	False		-26 18:37:39		N/A	Disabl
64	680	svchost.exe	0xe38ab88e3340	14		0	False		-26 18:37:40		N/A	Disabl
84	680	svchost.exe	0xe38ab84a3080	11		0	False	2023-12	-20 10.57:40	.000000	N/A N/A	DIZGDI

	600		0 30 1 001 1000			- 1	2022 42 25 40 27 42 20222	** / *	6' 13 1	
94	680	svchost.exe	0xe38ab89bd080	2	0	False	2023-12-26 18:37:42.000000	N/A	Disabled	
16	680	svchost.exe	0xe38ab89e3080	6	0	False	2023-12-26 18:37:42.000000	N/A	Disabled	
24	680	svchost.exe	0xe38ab89e4080	4	0	False	2023-12-26 18:37:42.000000	N/A	Disabled	
6	680	svchost.exe	0xe38ab89e6340	8	0	False	2023-12-26 18:37:43.000000	N/A	Disabled	
8	680	svchost.exe	0xe38ab891f340		0	False	2023-12-26 18:37:43.000000	N/A	Disabled	
4	2704	dasHost.exe	0xe38ab8911080		0	False	2023-12-26 18:37:43.000000	N/A	Disabled	
8	680	spoolsv.exe	0xe38ab8942300		0	False	2023-12-26 18:37:44.000000	N/A	Disabled	
8	680	svchost.exe	0xe38ab8946080	9	0	False	2023-12-26 18:37:44.000000	N/A	Disabled	
0	680	svchost.exe	0xe38ab893f080	6	0	False	2023-12-26 18:37:45.000000	N/A	Disabled	
8	680	svchost.exe		6	0	False	2023-12-26 18:37:47.000000	N/A	Disabled	
2	680	svchost.exe		14	0	False	2023-12-26 18:37:48.000000	N/A	Disabled	
2	680	svchost.exe	0xe38ab8bb5080	5	0	False	2023-12-26 18:37:48.000000	N/A	Disabled	
9	1392	sihost.exe	0xe38ab98b6080			False	2023-12-26 18:37:51.000000	N/A	Disabled	
2	680	svchost.exe	0xe38ab98be080			False	2023-12-26 18:37:52.000000	N/A	Disabled	
4	680	svchost.exe	0xe38ab98e4080			False	2023-12-26 18:37:52.000000	N/A	Disabled	
2	680	svchost.exe	0xe38ab98a4340			False	2023-12-26 18:37:53.000000	N/A	Disabled	
3	680	svchost.exe	0xe38ab990b340	10	0	False	2023-12-26 18:37:53.000000	N/A	Disabled	
9	680	svchost.exe	0xe38ab990a080	15	0	False	2023-12-26 18:37:53.000000	N/A	Disabled	
3	680	svchost.exe	0xe38ab990c080		0	False	2023-12-26 18:37:53.000000	N/A	Disabled	
)	680	svchost.exe	0xe38ab99b9080	2	0	False	2023-12-26 18:37:54.000000	N/A	Disabled	
	680	svchost.exe	0xe38ab99ca340			False	2023-12-26 18:37:55.000000	N/A	Disabled	
	680	svchost.exe	0xe38ab99c4240			False	2023-12-26 18:37:55.000000	N/A	Disabled	
	680	MsMpEng.exe	0xe38ab9a2c080	29	0	False	2023-12-26 18:37:55.000000	N/A	Disabled	
	680	svchost.exe	0xe38ab9a2e340		0	False	2023-12-26 18:37:56.000000	N/A	Disabled	
1	1248	updatechecker.		0		False	2023-12-26 18:37:56.000000		12-26 18:38:48.000000	Disabled
1	1248	taskhostw.exe	0xe38ab9a560c0	9		False	2023-12-26 18:37:56.000000	N/A	Disabled	
1	1248	taskhostw.exe	0xe38ab9a8f080	4		False	2023-12-26 18:37:56.000000	N/A	Disabled	
	1248	taskhostw.exe		0		False	2023-12-26 18:37:57.000000		12-26 18:38:08.000000	Disable
•	680	svchost.exe	0xe38ab9b3c080	3	0	False	2023-12-26 18:37:58.000000	N/A	Disabled	
	680	svchost.exe	0xe38ab9b55340	12	0	False	2023-12-26 18:37:59.000000	N/A	Disabled	
1	680	svchost.exe	0xe38ab9ba9080			False	2023-12-26 18:37:59.000000	N/A	Disabled	
	4204	ctfmon.exe	0xe38ab9c350c0	10		False	2023-12-26 18:38:01.000000	N/A	Disabled	
3	680	svchost.exe	0xe38ab9cf2080		Θ	False	2023-12-26 18:38:04.000000	N/A	Disabled	
9	680	svchost.exe	0xe38ab9e4d340			False	2023-12-26 18:38:09.000000	N/A	Disabled	
3	680	svchost.exe	0xe38ab9d1f080			False	2023-12-26 18:38:12.000000		12-26 18:44:25.000000	Disabled
	612	userinit.exe	0xe38ab9eb8080			False	2023-12-26 18:38:23.000000	2023-1	2-26 18:38:42.000000	Disabled
	1664	explorer.exe	0xe38ab9c1d080	55		False	2023-12-26 18:38:24.000000	N/A	Disabled	
	680	svchost.exe	0xe38ab9f91080			False	2023-12-26 18:38:30.000000	N/A	Disabled	
	3844	updatechecker.	0xe38aba198080	15		False	2023-12-26 18:38:36.000000	N/A	Disabled	
	804	TextInputHost.	0xe38ab9d1e080	11		False	2023-12-26 18:38:45.000000	N/A	Disabled	
	804	StartMenuExper	0xe38ab9cf3080	10		False	2023-12-26 18:38:45.000000	N/A	Disabled	
	804	RuntimeBroker.	0xe38ab8a1f2c0			False	2023-12-26 18:38:49.000000	N/A	Disabled	
	680	svchost.exe	0xe38ab842c340			False	2023-12-26 18:38:51.000000	N/A	Disabled	
	804	MoUsoCoreWorke	0xe38ab48d3080			False	2023-12-26 18:38:52.000000	N/A	Disabled	
	804	RuntimeBroker.	0xe38ab38d6240	10		False	2023-12-26 18:38:56.000000	N/A	Disabled	
	680	SearchIndexer.	0xe38ab4aae340	19	0	False	2023-12-26 18:38:57.000000	N/A	Disabled	
	680	NisSrv.exe	0xe38ab4ab62c0	4	0	False	2023-12-26 18:38:59.000000	N/A	Disabled	
	680	svchost.exe	0xe38aba3f4080		0	False	2023-12-26 18:39:04.000000	N/A	Disabled	
	768	SecurityHealth		3	1	False	2023-12-26 18:39:16.000000	N/A	Disabled	
1	680	SecurityHealth	0xe38ab49ba080	9	0	False	2023-12-26 18:39:16.000000	N/A	Disabled	
	768	VBoxTray.exe	0xe38ab49bb080		1	False	2023-12-26 18:39:17.000000	N/A	Disabled	

6800	768	msedge.exe	0xe38ab4c7e080	51	-	1	False	2023-12-26 18:39:19.000000	N/A	Disabled	
6896	3856	GoogleCrashHan	0xe38ab4c7a080			0	True	2023-12-26 18:39:23.000000	N/A	Disabled	
6924	6800	msedge.exe	0xe38abb5c90c0	8		1	False	2023-12-26 18:39:24.000000	N/A	Disabled	
7128	6800	msedge.exe	0xe38abb6ef0c0	15		1	False	2023-12-26 18:39:25.000000	N/A	Disabled	
7156	6800	msedge.exe	0xe38abb5860c0	16		1	False	2023-12-26 18:39:25.000000	N/A	Disabled	
3616	6800	msedge.exe	0xe38abb7020c0	8		1	False	2023-12-26 18:39:26.000000	N/A	Disabled	
6096	6800	msedge.exe	0xe38abb6f4300	17		1	False	2023-12-26 18:39:26.000000	N/A	Disabled	
6072	804	SearchApp.exe	0xe38aba37a080	47		1	False	2023-12-26 18:39:27.000000	N/A	Disabled	
7192	6800	msedge.exe	0xe38aba9ce280	14		1	False	2023-12-26 18:39:28.000000	N/A	Disabled	
7396	3856	GoogleCrashHan	0xe38abb7340c0			0	False	2023-12-26 18:39:30.000000	N/A	Disabled	
7480	680	svchost.exe	0xe38ab462d2c0	2		1	False	2023-12-26 18:39:53.000000	N/A	Disabled	
5696	680	svchost.exe	0xe38ab38d5080			0	False	2023-12-26 18:39:59.000000	N/A	Disabled	
6028	680	SgrmBroker.exe	0xe38abbd6e080			0	False	2023-12-26 18:40:01.000000	N/A	Disabled	
5244	680	svchost.exe	0xe38aba9e3080			0	False	2023-12-26 18:40:03.000000	N/A	Disabled	
8224	680	svchost.exe	0xe38abbc66080			0	False	2023-12-26 18:40:04.000000	N/A	Disabled	
8284	680	svchost.exe	0xe38aba9db080	4		0	False	2023-12-26 18:40:05.000000	N/A	Disabled	
8396	680	svchost.exe	0xe38abbc6b080	2		0	False	2023-12-26 18:40:07.000000	N/A	Disabled	
8440	680	svchost.exe	0xe38abbdd8080	4		0	False	2023-12-26 18:40:08.000000	N/A	Disabled	
8588	680	svchost.exe	0xe38aba9e2080	8		0	False	2023-12-26 18:40:09.000000	N/A	Disabled	
1804	804	PhoneExperienc	0xe38abb805080	17		1	False	2023-12-26 18:40:37.000000	N/A	Disabled	
8412	804	RuntimeBroker.	0xe38ab3621340	2		1	False	2023-12-26 18:40:41.000000	N/A	Disabled	
5980	680	svchost.exe	0xe38ab9c55080			0	False	2023-12-26 18:41:21.000000	N/A	Disabled	
4416	680	svchost.exe	0xe38abbce0080	0		0	False	2023-12-26 18:41:23.000000	2023-12	2-26 18:41:26.000000	Disabled
8924	804	RuntimeBroker.	0xe38ab491f080			1	False	2023-12-26 18:42:49.000000	N/A	Disabled	
1900	804	User00BEBroker	0xe38aba3dc080	4		1	False	2023-12-26 18:48:42.000000	N/A	Disabled	
2744	804	SystemSettings	0xe38abb576080	18		1	False	2023-12-26 18:53:03.000000	N/A	Disabled	
7172	804	ApplicationFra		4		1	False	2023-12-26 18:53:03.000000	N/A	Disabled	
0	0	0xe38ab	47f6080 0		N/A	False	N/A	N/A Disabled			

El primer comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: "python vol.py -f C:\Herramientas\windows_ram.mem windows.pslist.PsList"

El comando windows.pslist.PsList se utiliza para extraer y mostrar información sobre los procesos que estaban en ejecución en un sistema Windows en el momento en que se creó el volcado de memoria. Estos procesos pueden incluir aplicaciones y servicios que estaban activos en ese momento. Este análisis puede ser útil para investigar incidentes de seguridad, identificar procesos maliciosos o comprender la actividad del sistema en un momento específico.

Una de las cosas que podemos destacar de este análisis es la siguiente información "6896 3856 GoogleCrashHan 0xe38ab4c7a080 5 - 0 True 2023-12-26 18:39:23.000000 N/A Disabled"

Que es un comando que es un ping a Google.com que habíamos lanzado en el momento de la adquisición.

2.2 Windows.psscan.PsScan

		\volatility3-2.4	.0\volatility3-2	.4.0>pyt	hon vol.	py -f C:	\Herrami	entas\win	dows_ram.me	m windows.pss	can.PsS	can
	s: 100.		PDB scanning fi	nichad								
PID	PPID	ImageFileName	Offset(V)		Handles	Section	Td	Wow64	CreateTime	ExitTime		File outp
FIU	FFID	Tillagel TTelvalle	OTTSEC(V)	IIII eaus	Hallutes	26331011	Iu	WOW04	CI eate I IIIe	LXICIIII		Tite ouch
4	0	System 0xe38ab	1e83040 127		N/A	False	2023-12	-26 18:37	:01.000000	N/A	Disable	d
1584	680	svchost.exe	0xe38ab1e86080	6		0	False		26 18:37:33	.000000	N/A	Disabled
92	4	Registry	0xe38ab1fba040	4		N/A	False		26 18:36:34		N/A	Disabled
8412	804	RuntimeBroker.	0xe38ab3621340	2		1	False	2023-12-	26 18:40:41	.000000	N/A	Disabled
5696	680	svchost.exe	0xe38ab38d5080	3		0	False	2023-12-	26 18:39:59	.000000	N/A	Disabled
1084	804	RuntimeBroker.	0xe38ab38d6240	10		1	False	2023-12-	26 18:38:56	.000000	N/A	Disabled
348	4	smss.exe	0xe38ab3e7f040	2		N/A	False	2023-12-	26 18:37:01	.000000	N/A	Disabled
1688	680	svchost.exe	0xe38ab454d080	8		0	False	2023-12-	26 18:37:34	.000000	N/A	Disabled
612	536	winlogon.exe	0xe38ab4555080	6		1	False	2023-12-	26 18:37:24	.000000	N/A	Disabled
7480	680	svchost.exe	0xe38ab462d2c0	2		1	False	2023-12-	26 18:39:53	.000000	N/A	Disabled
2092	612	dwm.exe 0xe38ab			1	False			:47.000000	N/A	Disable	
5972	804	MoUsoCoreWorke	0xe38ab48d3080	7		0	False		26 18:38:52		N/A	Disabled
8924	804	RuntimeBroker.	0xe38ab491f080	7		1	False		26 18:42:49		N/A	Disabled
6584	680	SecurityHealth	0xe38ab49ba080	9		0	False		26 18:39:16		N/A	Disabled
6612	768	VBoxTray.exe	0xe38ab49bb080	11		1	False		26 18:39:17		N/A	Disabled
6552	768	SecurityHealth	0xe38ab49be080	3		1	False		26 18:39:16		N/A	Disabled
544	448	wininit.exe	0xe38ab4a80080	1		0	False		26 18:37:24		N/A	Disabled
680	544	services.exe	0xe38ab4a83140	10		0	False		26 18:37:25		N/A	Disabled
552	536	csrss.exe	0xe38ab4a85140	12		1	False		26 18:37:24		N/A	Disabled
2356	680	SearchIndexer.	0xe38ab4aae340	19		0	False		26 18:38:57		N/A	Disabled
4184	680	NisSrv.exe	0xe38ab4ab62c0	4		0	False		26 18:38:59		N/A	Disabled
928	680	svchost.exe	0xe38ab4c09080	18		0	False		26 18:37:28		N/A	Disabled
6896	3856	GoogleCrashHan	0xe38ab4c7a080	5		0	True		26 18:39:23		N/A	Disabled
3064	804	dllhost.exe	0xe38ab4c7b080	12		1	False		26 19:19:43		N/A	Disabled
6800	768	msedge.exe	0xe38ab4c7e080	51		1	False		26 18:39:19		N/A	Disabled
696	544	lsass.exe	0xe38ab4ca4080	12		0	False		26 18:37:25		N/A	Disabled
6188	680	svchost.exe	0xe38ab4ef3080	8		0	False		26 19:28:35		N/A	Disabled
460	448	csrss.exe	0xe38ab4f0b080	11		0	False		26 18:37:22		N/A	Disabled
1964	680	svchost.exe	0xe38ab4fe30c0	10		0	False		26 18:37:36		N/A	Disabled
980	680	svchost.exe	0xe38ab8224340	6 9		0	False		26 18:37:28		N/A	Disabled
5888 2584	680 680	svchost.exe	0xe38ab842c340	11		0 0	False False		26 18:38:51		N/A N/A	Disabled
	680	svchost.exe	0xe38ab84a3080	6		0	False		26 18:37:41		N/A N/A	Disabled Disabled
720 1032	680	svchost.exe	0xe38ab851d340	4		0	False False		26 18:37:30			Disabled
1032 1056	680	svchost.exe svchost.exe	0xe38ab85230c0	2		0	False		26 18:37:30		N/A N/A	Disabled
1040	680	svchost.exe	0xe38ab852a080 0xe38ab852b080	3		0	False		26 18:37:30 26 18:37:30		N/A N/A	Disabled
1108	680	svchost.exe	0xe38ab854a080	4		0	False		26 18:37:30 26 18:37:30		N/A N/A	Disabled
1228	680	svchost.exe	0xe38ab8581080	8		0	False		26 18:37:30 26 18:37:31		N/A N/A	Disabled
1228	680	svchost.exe	0xe38ab8584340	8 5		0	False		26 18:37:31 26 18:37:31		N/A N/A	Disabled
1248	680	svchost.exe	0xe38ab8587340	12	_	0	False		26 18:37:31 26 18:37:31		N/A N/A	Disabled
1332	680	svchost.exe	0xe38ab85b9080	5		0	False		26 18:37:31 26 18:37:31		N/A N/A	Disabled
1340	680	svchost.exe	0xe38ab85bc0c0	5		0	False		26 18:37:31 26 18:37:31		N/A	Disabled
1392	680	svchost.exe	0xe38ab8621340	7		0	False		26 18:37:31 26 18:37:31		N/A	Disabled
1444	680	svchost.exe	0xe38ab8627080	7		0	False		26 18:37:32		N/A	Disabled
1516	680	svchost.exe	0xe38ab86780c0	3		0	False		26 18:37:33		N/A	Disabled
2010	000	J. CHOJ C. CAC	0.0000000000000000000000000000000000000	_		-	, 4136	2023 12-	20 10:37:33	. 55555	,	DIJUDICU

1728	680	VBoxService.ex	0xe38ab86a3340	11	_	0	False	2023-12-26 18:37:35.000000	N/A	Disabled	
804	680	svchost.exe		15		ē	False	2023-12-26 18:37:27.000000	N/A	Disabled	
828	612	fontdrvhost.ex	0xe38ab8742240			1	False	2023-12-26 18:37:28.000000	N/A	Disabled	
836	544	fontdrvhost.ex	0xe38ab8744240	5		ē	False	2023-12-26 18:37:28.000000	N/A	Disabled	
2140	680	svchost.exe	0xe38ab88720c0			ø	False	2023-12-26 18:37:37.000000	N/A	Disabled	
2148	680	svchost.exe		3		0	False	2023-12-26 18:37:37.000000	N/A	Disabled	
2168	680	svchost.exe		2		0	False	2023-12-26 18:37:38.000000	N/A	Disabled	
2216	680	svchost.exe		11		0	False	2023-12-26 18:37:38.000000	N/A	Disabled	
2336	680	svchost.exe	0xe38ab88a0080	5		0	False	2023-12-26 18:37:39.000000	N/A	Disabled	
2464	680	svchost.exe		14		0	False	2023-12-26 18:37:40.000000	N/A	Disabled	
2864	2704	dasHost.exe	0xe38ab8911080			0	False	2023-12-26 18:37:43.000000	N/A	Disabled	
2808	680	svchost.exe		3		0	False	2023-12-26 18:37:43.000000	N/A	Disabled	
3000	680	svchost.exe		6		0	False	2023-12-26 18:37:45.000000	N/A	Disabled	
2928	680	spoolsv.exe	0xe38ab8942300			0	False	2023-12-26 18:37:44.000000	N/A	Disabled	
2968	680	svchost.exe	0xe38ab8946080	9		0	False	2023-12-26 18:37:44.000000	N/A	Disabled	
2704	680	svchost.exe	0xe38ab89bd080			0	False	2023-12-26 18:37:42.000000	N/A	Disabled	
2716	680	svchost.exe	0xe38ab89e3080	6		0	False	2023-12-26 18:37:42.000000	N/A	Disabled	
2724	680	svchost.exe		4		0	False	2023-12-26 18:37:42.000000	N/A	Disabled	
2736	680	svchost.exe		8		0	False	2023-12-26 18:37:43.000000	N/A	Disabled	
5788	804	RuntimeBroker.	0xe38ab8a1f2c0	3		1	False	2023-12-26 18:38:49.000000	N/A	Disabled	
1876	680	svchost.exe	0xe38ab8a22080	2		0	False	2023-12-26 18:37:35.000000	N/A	Disabled	
1920	680	svchost.exe	0xe38ab8a7d080	5		0	False	2023-12-26 18:37:36.000000	N/A	Disabled	
1928	680	svchost.exe	0xe38ab8a7f0c0	9		0	False	2023-12-26 18:37:36.000000	N/A	Disabled	
1948	680	svchost.exe		4		ø	False	2023-12-26 18:37:36.000000	N/A	Disabled	
1408	4	MemCompression		26		N/A	False	2023-12-26 18:37:37.000000	N/A	Disabled	
1564	680	svchost.exe	0xe38ab8abf340	2		0	False	2023-12-26 18:37:37.000000	N/A	Disabled	
2076	680	svchost.exe	0xe38ab8ac0080	3		0	False	2023-12-26 18:37:37.000000	N/A	Disabled	
2228	680	svchost.exe	0xe38ab8ba0340	6		0	False	2023-12-26 18:37:47.000000	N/A	Disabled	
2772	680	svchost.exe		14		ē	False	2023-12-26 18:37:48.000000	N/A	Disabled	
3092	680	svchost.exe	0xe38ab8bb5080	5		0	False	2023-12-26 18:37:48.000000	N/A	Disabled	
3532	680	svchost.exe	0xe38ab98a4340			ø	False	2023-12-26 18:37:53.000000	N/A	Disabled	
3340	1392	sihost.exe		12		1	False	2023-12-26 18:37:51.000000	N/A	Disabled	
3372	680	svchost.exe	0xe38ab98be080	9		1	False	2023-12-26 18:37:52.000000	N/A	Disabled	
3504	680	svchost.exe	0xe38ab98e4080	6		1	False	2023-12-26 18:37:52.000000	N/A	Disabled	
3560	680	svchost.exe	0xe38ab990a080	15		0	False	2023-12-26 18:37:53.000000	N/A	Disabled	
3548	680	svchost.exe	0xe38ab990b340	10		0	False	2023-12-26 18:37:53.000000	N/A	Disabled	
3568	680	svchost.exe	0xe38ab990c080			0	False	2023-12-26 18:37:53.000000	N/A	Disabled	
3660	680	svchost.exe	0xe38ab99b9080			0	False	2023-12-26 18:37:54.000000	N/A	Disabled	
3696	680	svchost.exe	0xe38ab99c4240			0	False	2023-12-26 18:37:55.000000	N/A	Disabled	
3672	680	svchost.exe	0xe38ab99ca340	6		0	False	2023-12-26 18:37:55.000000	N/A	Disabled	
3712	680	MsMpEng.exe	0xe38ab9a2c080	29		0	False	2023-12-26 18:37:55.000000	N/A	Disabled	
3736	680	svchost.exe	0xe38ab9a2e340			0	False	2023-12-26 18:37:56.000000	N/A	Disabled	
3844	1248	updatechecker.	0xe38ab9a53080	0			False	2023-12-26 18:37:56.000000	2023-12	-26 18:38:48.000000	Disabled
3864	1248	taskhostw.exe	0xe38ab9a560c0				False	2023-12-26 18:37:56.000000	N/A	Disabled	
3904	1248	taskhostw.exe					False	2023-12-26 18:37:56.000000	N/A	Disabled	
6232	680	svchost.exe	0xe38ab9a96080				False	2023-12-26 19:24:19.000000	N/A	Disabled	
3996	1248	taskhostw.exe	0xe38ab9adb0c0				False	2023-12-26 18:37:57.000000	2023-12	-26 18:38:08.000000	Disabled
4080	680	svchost.exe	0xe38ab9b3c080				False	2023-12-26 18:37:58.000000	N/A	Disabled	
4152	680	svchost.exe		12			False	2023-12-26 18:37:59.000000	N/A	Disabled	
2776	5720	chrome.exe	0xe38ab9b9f080				False	2023-12-26 19:24:32.000000	N/A	Disabled	
4204	680	svchost.exe	0xe38ab9ba9080				False	2023-12-26 18:37:59.000000	N/A	Disabled	
		•									

El segundo comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: "python vol.py -f C:\Herramientas\windows_ram.mem windows.psscan.PsScan"

Este comando está diseñado para escanear la memoria en busca de información sobre procesos.

Es útil para obtener una vista más detallada y extensa de la información del proceso en comparación con el comando pslist. Puedes usarse para realizar un análisis más profundo de los procesos presentes en un volcado de memoria y obtener información adicional, como detalles de seguridad y tiempo de CPU utilizado.

```
"7796 5720 chrome.exe 0xe38abb782080 15 - 1 False 2023-12-26 19:24:33.000000 N/A Disabled"

"7860 768 notepad++.exe 0xe38abb785080 5 - 1 False 2023-12-26 19:24:51.000000 N/A Disabled"
```

Podemos destacar estos dos procesos que había activado en el sistema en el momento en el que creé el volcado de sistema.

2.3 Windows.pstree.PsTree

	as\volatility3-2.4	1.0\volatility3-2	.4.0>pyt	thon vo	ol.py -f	C:\Herrami	ientas\window	s_ram.men	ı windo	ws.pstree.	sTree
Volatility 3 Progress: 10 PID PPID	Framework 2.4.0 0.00 ImageFileName	PDB scanning fir Offset(V)		s Handl	es Sessi	ionId	Wow64 Cre	ateTime	Ext	itTime	
4 0	System 0xe38ab			N/A	False	2023-12	2-26 18:37:01	.000000	N/A	A	
* 1408 4 * 92 4	MemCompression Registry	0xe38ab1fba040	26 4		N/A N/A	False False	2023-12-26 2023-12-26			N/A N/A	
* 348 4 460 448	smss.exe csrss.exe	0xe38ab3e7f040 0xe38ab4f0b080	2 11		N/A 0	False False	2023-12-26 2023-12-26			N/A N/A	
544 448 * 680 544	wininit.exe services.exe	0xe38ab4a80080 0xe38ab4a83140	1 10		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
** 1032 680 ** 1040 680	svchost.exe svchost.exe	0xe38ab85230c0 0xe38ab852b080	4		9	False False	2023-12-26	18:37:30.	000000	N/A N/A	
** 3092 680 ** 2584 680	svchost.exe	0xe38ab8bb5080	5 11		9	False False	2023-12-26 2023-12-26 2023-12-26	18:37:48.	000000	N/A N/A	
** 1564 680	svchost.exe svchost.exe	0xe38ab84a3080 0xe38ab8abf340			0	False	2023-12-26	18:37:37.	000000	N/A	
** 1056 680	svchost.exe svchost.exe	0xe38ab8ac0080 0xe38ab852a080	3 2		0	False False	2023-12-26 2023-12-26	18:37:30.	000000	N/A N/A	
** 8224 680 ** 1584 680	svchost.exe svchost.exe	0xe38abbc66080 0xe38ab1e86080	5 6		0 0	False False	2023-12-26 2023-12-26	18:37:33.	000000	N/A N/A	
** 4152 680 ** 5696 680	svchost.exe svchost.exe	0xe38ab9b55340 0xe38ab38d5080	12 3		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
** 3660 680 ** 1108 680	svchost.exe svchost.exe	0xe38ab99b9080 0xe38ab854a080	2		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
** 3672 680 ** 4184 680	svchost.exe NisSrv.exe	0xe38ab99ca340 0xe38ab4ab62c0	6 4		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
** 2140 680 ** 4188 680	svchost.exe svchost.exe	0xe38ab88720c0 0xe38aba3f4080	6 5		9	False False	2023-12-26 2023-12-26	18:37:37.	000000	N/A N/A	
** 8284 680	svchost.exe	0xe38aba9db080	4		9	False	2023-12-26	18:40:05.	000000	N/A	
** 4204 680	svchost.exe svchost.exe	0xe38ab8877080 0xe38ab9ba9080	3 4		0	False False	2023-12-26 2023-12-26	18:37:59.	000000	N/A N/A	
*** 4376 ** 3696 680	4204 ctfmon. svchost.exe	0xe38ab99c4240		10	9	1 False	2023-12-26		000000	N/A	N/A
** 2168 680 ** 5244 680	svchost.exe svchost.exe	0xe38ab887b0c0 0xe38aba9e3080	9		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
** 3712 680 ** 2704 680	MsMpEng.exe svchost.exe	0xe38ab9a2c080 0xe38ab89bd080	29 2		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
*** 2864 ** 1688 680	2704 dasHost svchost.exe	t.exe 0xe38ab8 0xe38ab454d080	8911080 8		9	0 False	False 202 2023-12-26	3-12-26 1 18:37:34.		3.000000 N/A	N/A
** 3736 680 ** 2716 680	svchost.exe svchost.exe	0xe38ab9a2e340 0xe38ab89e3080	7		9	False False	2023-12-26 2023-12-26	18:37:56.	000000	N/A N/A	
** 2724 680 ** 2216 680	svchost.exe svchost.exe	0xe38ab89e4080 0xe38ab88830c0	4 11		9	False False	2023-12-26 2023-12-26 2023-12-26	18:37:42.	000000	N/A N/A	
** 2736 680	svchost.exe	0xe38ab89e6340	8		0	False	2023-12-26	18:37:43.	000000	N/A	
** 1728 680	svchost.exe VBoxService.ex		6 11		0	False False	2023-12-26 2023-12-26	18:37:35.	000000	N/A N/A	
** 4800 680 ** 1228 680	svchost.exe svchost.exe	0xe38ab9e4d340 0xe38ab8581080	6 8		0	False False	2023-12-26 2023-12-26	18:37:31.	000000	N/A N/A	
** 8396 680 ** 720 680	svchost.exe svchost.exe	0xe38abbc6b080 0xe38ab851d340	2 6		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
** 2772 680 ** 1240 680	svchost.exe svchost.exe	0xe38ab8ba62c0 0xe38ab8584340	14 5		0 0	False False	2023-12-26 2023-12-26			N/A N/A	
** 1248 680 *** 3864	svchost.exe 1248 taskhos	0xe38ab8587340 stw.exe 0xe38ab9	12 9a560c0		0 -	False 1	2023-12-26 False 202	18:37:31. 3-12-26 1		N/A 5.000000	N/A
*** 3996 *** 3994	1248 taskhostw.ex		0	-	1		23-12-26 18:37:			3-12-26 18:3	8:08.00000
*** 3904 *** 3844 **** 5276	1248 taskhostw.ex 1248 updatechecke 3844 updatechecke	er. 0xe38ab9a53080	4 0 15		1 1 1	False 202	23-12-26 18:37: 23-12-26 18:37: 23-12-26 18:38:	56.000000	N/A 202 N/A	3-12-26 18:3	8:48.000000
** 2808 680 ** 8440 680	svchost.exe 0xe	38ab891f340 3 38abbdd8080 4		0 0	False False	2023-12-26	18:37:43.00000 18:40:08.00000	0 N/A			
** 5888 680 ** 2336 680	svchost.exe 0xe	38ab842c340 9 38ab88a0080 5		0	False False	2023-12-26	18:38:51.00000 18:37:39.00000	0 N/A			
** 804 680 *** 5568 *** 8924	804 StartMenuExp	38ab873a340 15 per 0xe38ab9cf3080 er. 0xe38ab491f080	10 7		False 1 1	False 202	18:37:27.00000 3-12-26 18:38: 3-12-26 18:42:	45.000000	N/A N/A		
*** 7172 *** 1804	804 Application 804 PhoneExperie	Fra 0xe38abb74f080	4 17		1	False 202	23-12-26 18:53: 23-12-26 18:40:	03.000000	N/A N/A		
*** 1900 *** 1084	804 UserOOBEBrok 804 RuntimeBrok	ker 0xe38aba3dc080 er. 0xe38ab38d6240	4 10			False 202 False 202	23-12-26 18:48: 23-12-26 18:38:	42.000000 56.000000	N/A N/A		
*** 2744 *** 8412	804 SystemSettir 804 RuntimeBroke	er. 0xe38ab3621340	18 2			False 202	23-12-26 18:53: 23-12-26 18:40:	41.000000	N/A N/A		
*** 5972 *** 6072 *** 5560	804 MoUsoCoreWor 804 SearchApp.ex	xe 0xe38aba37a080	7 47 11		0		23-12-26 18:38: 23-12-26 18:39:	27.000000	N/A N/A N/A		
*** 5560 *** 5788 ** 3372 680	804 TextInputHos 804 RuntimeBroke sychost.exe 0xe		3		1			45.000000			
** 1332 680 ** 2356 680					1	False 202 False 202	23-12-26 18:38: 23-12-26 18:38:	49.000000	N/A		
** 7480 680	svchost.exe 0xe	38ab98be080 9 38ab85b9080 5		1 0	False False	False 202 False 202 2023-12-26 2023-12-26	23-12-26 18:38: 23-12-26 18:38: 18:37:52.00000 18:37:31.00000	49.000000 0 N/A 0 N/A			
** 1340 680	svchost.exe 0xe SearchIndexer. 0xe svchost.exe 0xe	38ab98be080 9			False	False 202 False 202 2023-12-26 2023-12-26 2023-12-26 2023-12-26	23-12-26 18:38: 23-12-26 18:38: 18:37:52.00000	49.000000 0 N/A 0 N/A 0 N/A 0 N/A			
** 1340 680 ** 4416 680 ** 1876 680	svchost.exe 0xe SearchIndexer. 0xe svchost.exe 0xe svchost.exe 0xe svchost.exe 0xe svchost.exe 0xe	38ab98be080 9 38ab85b9080 5 38ab4aae340 19 38ab462d2c0 2 38ab85bc0c0 5 38ab8ce0880 0 38ab8a22080 2		1 0 0 1 0 0	False False False False False False False	False 202 False 202 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26	23-12-26 18:38: 23-12-26 18:38: 18:37:52.00000 18:37:31.00000 18:38:57.00000 18:39:53.00000 18:37:31.00000 18:41:23.000000 18:37:35.000000	49.000000 0 N/A 0 N/A 0 N/A 0 N/A 0 N/A 0 202 0 N/A	N/A		000
** 1340 680 ** 4416 680 ** 1876 680 ** 5980 680 ** 4968 680	svchost.exe 0xes SearchIndexer. 0xes svchost.exe 0xes svchost.exe 0xes svchost.exe 0xes svchost.exe 0xes svchost.exe 0xes svchost.exe 0xes	38ab98be880 9 38ab4sae340 19 38ab45d2d2c0 2 38ab45bc0c0 5 38ab8c0e0880 0 38ab8a22880 2 38ab9d1f0880 0		1 0 1 0 0 0	False	False 202 False 202 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26	13-12-26 18:38: 13-12-26 18:38: 18:37:52.00000 18:37:31.00000 18:38:57.00000 18:39:53.00000 18:37:31.00000 18:41:23.00000 18:41:21.00000 18:41:21.00000	49.000000 0 N/A	N/A 3-12-26		
** 1340 680 ** 4416 680 ** 1876 680 ** 5980 680 ** 4968 680 ** 1392 680 *** 3340	svchost.exe 0xe SearchIndexer. 0xe svchost.exe 0xe 1392 sihost.exe	38ab98be886 9 3 38ab48ab946 5 38ab44aas340 19 38ab462d2c0 2 38ab85bce06 5 38abbce0880 0 38ab8a22880 2 38ab94556880 3 38ab941f688 0 38ab8621340 7 0xc33ab98b688	12	1 0 1 0 0 0 0 0	False False False False False False False False False	False 202 False 202 False 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 False 202	13-12-26 18:38: 13-12-26 18:39: 18:37:52.00000 18:37:31.00000 18:38:57.00000 18:39:53.00000 18:37:31.00000 18:41:23.00000 18:41:21.00000 18:41:21.00000 18:37:35.00000 18:37:37.31.00000	49.000000 N/A	N/A 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 4416 680 ** 1876 680 ** 5980 680 ** 4968 680 ** 1392 680 ** 3340 ** 2928 680 ** 1920 680	svchost.exe &xe: SearchIndexer. &xe: svchost.exe &xe: spoolsv.exe &xe: svchost.exe &xe:	38ab98be880 9 3 38ab85b9880 5 38ab43aa2340 19 38ab462d2c0 2 38ab85bce0 5 38abbce0880 0 38ab9822980 2 38ab96259880 3 38ab941f980 3 38ab9811440 7 6wc38ab98b680 38ab8841340 7 38ab8871490 5		1 0 0 0 0 0 0 0 0 0 0 0	False	False 202 False 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26	13-12-26 18:38: 18:37:52.00000 18:37:31.00000 18:38:57.00000 18:38:57.00000 18:39:53.00000 18:37:35.00000 18:41:23.00000 18:41:21.00000 18:41:21.00000 18:37:35.00000 18:37:35.00000 18:37:37.00000 18:37:37.00000	49.000000 0 N/A 0 N/A 0 N/A 0 N/A 0 N/A 0 N/A 0 202: 0 N/A 0 N/A 51.000000 0 N/A	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 4416 680 ** 1876 680 ** 5980 680 ** 4968 680 ** 1392 680 *** 3340 ** 2928 680	svchost.exe &xe: SearchIndexer &xe: svchost.exe &xe: sychost.exe &xe: spoolsv.exe &xe: svchost.exe &xe: sychost.exe &xe:	38ab98be880 9 3 38ab4aae340 19 3 38ab4aae340 19 3 38ab45ce0 5 5 38abbce0880 9 3 38ab825ce0880 2 38ab9c55880 3 38ab8621340 7 38ab842340 7	- - - - - - - - - - - - - - - - - - -	1 0 0 0 0 0 0 0 0 0	False	False 202 False 202 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26 2023-12-26	13-12-26 18:38: 13:37:52.00000 18:37:51.00000 18:38:57.00000 18:39:53.00000 18:37:31.00000 18:37:31.00000 18:37:35.00000 18:41:23.00000 18:41:21.00000 18:38:12.00000 18:38:12.00000 18:38:12.00000 18:38:12.100000	49.000000 N/A	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 19876 680 ** 5980 680 ** 1992 680 ** 1392 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 628 680 ** 8588 680 ** 1948 680	svchost.exe &xe: SearchIndexer. &xe: svchost.exe &xe:	38ab98be889 9 38ab85be889 5 38ab4aae340 19 38ab462d2c0 2 38ab85be6c0 5 38abb82d2880 2 38ab96c55880 3 38ab96f16880 0 38ab8621340 7 6xe38ab98be80 5 38ab8842300 7 38ab8a76c0 9 38ab8842300 7 38ab8a76800 7 38ab8a76800 7 38ab846880 5		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 2023-12-26	13-12-26 18:38: 13-12-26 18:38: 18:37:52, eeeeee 18:37:51, eeeeeee 18:39:51, eeeeeeee 18:39:53, eeeeeeeeeee 18:39:53, eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	49.000000 N/A 0 N/A	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 5980 680 ** 4968 680 ** 1392 680 ** 1392 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 2464 680	svchost.exe &xe: SearchIndexer. &xe: svchost.exe &xe:	38ab98be889 9 38ab48ab989 5 38ab4aae340 19 38ab462d20 2 38ab85bc0c0 5 38ab85bc0c0 6 38ab862d880 2 38ab961f680 0 38ab8621340 7 6xe38ab98b6980 5 38ab8621340 7 38ab8621340 7 38ab8621340 7 38ab8621340 7 38ab8621340 7 38ab8621340 1		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 2023-12-26	13-12-26 18:38: 13-12-26 18:38: 13-13-52, eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	49.000000 N/A 0 N/A	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 5980 680 ** 4968 680 ** 1392 680 ** 1292 680 ** 1292 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 2968 680 ** 1948 680 ** 2464 680 ** 1444 680 ** 1944 680	svchost.exe &xe. SearchIndexer &xe. svchost.exe &xe.	38ab98be880 9 38ab45ae340 19 38ab46c/d2c0 2 38ab45c0c0 5 38abbcc0880 0 38ab85c0c0 5 38abbcc0880 0 38ab8621340 7 38ab8621340 7 38ab8842340 7 38ab8842340 7 38ab8863340 14 38ab8863340 14 38ab8627880 17		100100000000000000000000000000000000000	False	False 202 2023-12-26	13-12-26 18:38: 18:37:52.00000 18:37:31.000000 18:37:31.000000 18:38:57.000000 18:38:57.000000 18:39:53.0000000 18:39:53.0000000 18:41:21.000000 18:41:21.000000 18:38:37:36.000000 18:38:37:36.000000 18:38:37:36.000000 18:38:37:36.000000 18:38:37:36.000000000000000000000000000000000000	49.000000 00 N/A	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 5980 680 ** 4968 680 ** 3340 ** 2928 680 ** 1922 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 2968 680 ** 2968 680 ** 2464 680 ** 1944 680 ** 1964 680 ** 1964 680 ** 1964 680 ** 1964 680	svchost.exe &xe: SearchIndexer &xe: svchost.exe &xe:	38ab98be889 9 38ab4aae340 19 38ab46c024c0 2 38ab46c0e0 5 38abbce0880 0 38ab86c060 5 38abbcc0880 0 38ab86c1340 7 38ab86c1340 7 38ab86c76c0 9 38ab86c76c0 9 38ab86c76c0 9 38ab86c76c0 9 38ab86c6800 7 38ab86c76c0 9 38ab86c76c0 10 38ab96c76c0 10		1001000000-000000000011	False	False 202 2023 12 26	13-12-26 18:38: 13-12-26 18:38: 18:37:52.00000 18:37:52.00000 18:37:51.00000 18:38:57.000000 18:38:57.000000 18:38:57.000000 18:38:57.000000 18:38:57.000000 18:38:57.0000000 18:38:57.56.000000 18:38:57.56.000000 18:37:56.000000 18:37:56.000000 18:37:56.0000000 18:37:56.000000000000000000000000000000000000	49.000000 0	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 1876 680 ** 1982 680 ** 4968 680 ** 1392 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1988 680 ** 2968 680 ** 1944 680 ** 1444 680 ** 1444 680 ** 5636 680	svchost.exe & &xe: SearchIndexer & &xe: Svchost.exe	38ab98be880 9 38ab4aae340 19 38ab46c02420 2 38ab46c060 5 38abbece980 0 38ab86c060 5 38abbece980 0 38ab8621340 7 38ab8621340 7 38ab862780 5 38ab862680 7 38ab862680 7 38ab884680 9 38ab884680 9 38ab884680 18 38ab886340 4 38ab86340 18		100100000000000000000000000000000000000	False	False 202 2023-12-26	13-12-26 18:38: 18:37:52, 0000001 18:37:51, 0000001 18:39:53, 0000001 18:39:53, 0000001 18:39:53, 0000001 18:40:53, 0000001 18:41:23, 0000001 18:41:23, 0000001 18:41:21, 0000001 18:41:26, 0000001 18:41:26, 0000001 18:41:26, 0000001 18:41:26, 0000001 18:41:26, 0000001 18:37:36, 0000001 18:37:36, 0000001 18:37:36, 0000001 18:37:36, 0000001 18:37:36, 0000001 18:37:36, 0000001 18:37:36, 0000001 18:37:36, 0000001	49.000000 0	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 968 680 ** 4968 680 ** 1392 680 ** 1922 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 1948 680 ** 2988 680 ** 1948 680 ** 1444 680 ** 1444 680 ** 1444 680 ** 1586 680 ** 1586 680 ** 1586 680 ** 1586 680 ** 1586 680 ** 1584 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3504 680	svchost.exe & &xe: SearchIndexer & &xe: svchost.exe	38ab98be889 9 38ab4aae340 19 38ab4abe02d2ce 2 38ab4ace040 5 38abb8ce080 6 38ab8b8ce080 6 38ab8622880 2 38ab9655880 3 38ab8621340 7 38ab8342300 7 38ab8347680 5 38ab8946880 9 38ab884680 9 38ab884680 9 38ab884680 14 38ab8863340 18 38ab8863340 18 38ab8863340 18 38ab863340 18 38ab86340 18 38ab86340 18 38ab86340 18 38ab86340 18		1001000000000000000011000000	False False	False 202 2023-12-26	3-12-26 18:38:38:31-12-26 18:38:18:37-52, 000000018:37-52, 00000018:37-52, 00000018:37-53, 000000018:37-53, 000000018:37-53, 000000018:37-53, 000000018:37-53, 000000018:37-53, 000000018:37-53, 000000018:37-53, 000000000000000000000000000000000000	49.000000 0 N/A	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 9968 680 ** 4968 680 ** 1392 680 ** 1922 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 2968 680 ** 2968 680 ** 1444 680 ** 1444 680 ** 1444 680 ** 1536 680 ** 3584 680 ** 3584 680 ** 3584 680 ** 3584 680 ** 3584 680 ** 3584 680 ** 3584 680 ** 3584 680 ** 3584 680 ** 3584 680	svchost.exe & &xe: SearchIndexer & &xe: Svchost.exe	38ab98be889 9 38ab485be889 5 38ab4aae340 19 38ab466240 6 2 38ab85bc0c0 5 38ab466260 6 3 38ab8621340 7 6xe38ab98621340 7 38ab8621340 8 38ab8621340 8 38ab8621340 9 38ab8621340 1 38ab8621340 1 38ab8621340 7 38ab8621340 7 38ab9621340 6 38ab9621340 7		10010000000000000000110000000	False	False 202 2023-12-26	13-12-26 18:38: 13-12-26 18:38: 18:37-52.00000 18:37-52.00000 18:37-52.00000 18:38-53.000000 18:38-53.000000 18:38-53.000000 18:38-53.000000 18:38-53.000000 18:38-53.000000 18:38-53.000000 18:38-53.000000 18:38-53.00000000 18:38-53.000000000000000000000000000000000000	49.000000 0	N/A 3-12-26 3-12-26	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 1987 680 ** 4968 680 ** 4968 680 ** 3340 ** 1922 680 ** 1922 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 2688 680 ** 2464 680 ** 1944 680 ** 1944 680 ** 1954 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3505 680 ** 3560 680 ** 3560 680 ** 3560 680 ** 3560 680 ** 3560 680	svchost.exe öxe: SearchIndexn öxe: svchost.exe öxe: sychost.exe öxe:	38ab98be880 9 38ab4aae340 19 38ab4ace340 19 38ab4ace340 2 38ab4ace340 5 38abbece9880 6 38ab8ece9880 2 38ab9ece9880 2 38ab9ece9880 7 38ab8ace340 7 38ab8ace340 9 38ab84ace340 9 38ab84ace340 9 38ab4ace340 9 38ab4ace340 1		100100000000000000000011000000000000000	False	False 202 2023-12-26	3-12-26 18:38:38:31-12-26 18:38:18:37:52.00000018:37:52.00000018:37:52.00000018:38:57.52.00000018:38:57.52.00000018:38:57.52.00000018:38:57.52.00000018:37:53.00000018:37:53.000000000000000000000000000000000000	49.000000 00 N/A	N/A 3-12-26 3-12-26 N/A	18:41:26.000 18:44:25.000	
** 1340 680 ** 1476 680 ** 1476 680 ** 1476 680 ** 1580 680 ** 1592 680 ** 1592 680 ** 1592 680 ** 1592 680 ** 1592 680 ** 1592 680 ** 1592 680 ** 1598 680 ** 1598 680 ** 1598 680 ** 1596 680 ** 1444 680 ** 1444 680 ** 1444 680 ** 1596 680 ** 1586 680 ** 3534 680 ** 3534 680 ** 3532 680 ** 3536 680 ** 3536 680 ** 4808 680 ** 3536 680 ** 4808 680 ** 3536 680 ** 4808 680 ** 3536 680	svchost.exe & &xe: svchost.exe &	38ab98be889 9 9 9 9 38ab88be889 5 38ab4ae348 0 9 9 9 9 9 8 9 9 9 9 9 9 9 9 9 9 9 9		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 7 False	3-12-26 18:38: 3-12-26 18:38: 3-12-26 18:38: 3-13-26 18:38: 3-13-16.000000 18:39-53.000000 18:39-53.000000 18:39-53.000000 18:39-53.000000 18:41-23.000000 18:41-23.000000 18:41-21.000000 18:41-21.000000 18:41-21.000000 18:41-21.000000 18:41-21.000000 18:37-36.000000	49.000000 19.0000000 10.000000000000000	N/A 3-12-26 3-12-26 N/A N/A	18:41:26.000 18:44:25.000	
** 1340 680 ** 1876 680 ** 1876 680 ** 1980 680 ** 4968 680 ** 1392 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 1948 680 ** 1944 680 ** 1444 680 ** 1444 680 ** 1444 680 ** 1564 680 ** 1566 680 ** 3586 680	svchost.exe & &xe: SearchIndexer & &xe: SearchIndexer & &xe: Svchost.exe & &xe: svchost.e	38ab98be889 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9		1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 2023-12-26 2	3-12-26 18:38: 3-12-26 18:38: 18:37:52, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:53, 0000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 0000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 0000000 18:39:53, 000000000000000000000000000000000000	49.000000 N/A N/A N/A N/A N/A N/A N/	N/A 3-12-26 3-12-26 N/A N/A N/A N/A N/A	18:41:26.000 18:44:25.000	
** 1340 680 ** 1476 680 ** 1476 680 ** 14968 680 ** 14968 680 ** 1392 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 1948 680 ** 2686 680 ** 2686 680 ** 2686 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 3586 680 ** 4088 680 ** 4588 680 ** 5586 680 ** 4088 680 ** 4588 680 ** 4588 680 ** 5586 680 ** 4088 680 ** 4088 680 ** 4088 680 ** 5596 544 552 536 612 536	svchost.exe öxe: scarchIndexer öxe: svchost.exe öxe:	38ab98be889 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 2023-12-26 2	3-12-26 18:38: 3-12-26 18:38: 18:37:52, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:53, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 000000 18:39:53, 000000000000000000000000000000000000	49.000000 49.000000 N/A 0 N/A	N/A 3-12-26 3-12-26 N/A N/A N/A N/A N/A N/A	18:41:26.000 18:44:25.000	999
** 1340 680 ** 1876 680 ** 1876 680 ** 4968 680 ** 4968 680 ** 1392 680 ** 1922 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1953 680 ** 1968 680 ** 1968 680 ** 1968 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3568 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 1966 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 4080 680 ** 3568 680 ** 4080 680 ** 4080 680 ** 3568 680 ** 4080 680	svchost.exe oxes sychost.exe oxes sychos	38aby8be888 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9		100110000000000000000000000000000000000	False	False 202 2023-12-26 2	3-12-26 18:38: 3-12-26 18:38: 18:37:52, 00000 18:39:53, 000000 18:39:54, 000000 18:39:54, 000000 18:39:54, 0000000 18:39:54, 000000000000000000000000000000000000	49.000000 49.000000 10	N/A 3-12-26 N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	18:41:26.006 18:44:25.006 3-12-26 18:	999
** 1340 680 ** 1476 680 ** 1476 680 ** 14968 680 ** 19968 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1994 680 ** 1948 680 ** 2668 680 ** 1948 680 ** 2464 680 ** 1944 680 ** 1444 680 ** 1444 680 ** 1593 680 ** 1593 680 ** 1593 680 ** 1593 680 ** 1593 680 ** 1593 680 ** 1593 680 ** 1516 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3504 680 ** 3505 680 ** 1516 680 ** 3566 680 ** 1516 680 ** 3566 680 ** 4080 680	svchost.exe öxe: searchIndexer öxe: svchost.exe öxe:	38aba98be889 9 9 9 38aba88be889 5 38ab4ae340 19 38ab85bc0e0 5 5 38abbece0889 2 38abb85bc0e0 5 5 38abb85bc0e0 6 5 38ab8621340 7 38ab8621340 7 38ab8621340 7 38ab8627680 19 38ab962680 6 38ab962680 6 38ab962680 6 38ab962680 6 38ab962680 7 38ab8627680 6 38ab962680 6 38ab962680 6 38ab962680 7 38ab8627680 7 38ab8627680 6 38ab962680 6 38ab962680 6 38ab962680 6 38ab962680 7 38ab8627680 9 38ab8627680 9 3 38ab8627680 9 3 38ab8627680 9 3 38ab8627680 9 3 38ab8627800 9 3 38ab8627800 9 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 False 202 False 2023-12-26 2023-12	3-12-26 18:38: 3-12-26 18:38: 18:37:52.00000 18:38:57.00000 18:38:57.00000 18:38:57.00000 18:38:57.00000 18:38:57.00000 18:38:57.00000 18:38:57.00000 18:38:57.00000 18:37:31.00000 18:37:31.00000 18:37:31.00000 18:37:31.00000 18:37:31.00000 18:37:31.00000 18:37:31.00000 18:37:36.00000 18:37:26.00000 18:37:26.00000 18:37:26.00000 18:37:26.00000 18:37:26.00000 18:37:26.00000	49.000000 49.000000 N/A 00 N/A	N/A 3-12-26 N/A N/A N/A N/A N/A N/A N/A N/A N/A 000000	18:41:26.006 18:44:25.006 3-12-26 18: N/A N/A N/A	999
** 1340 680 ** 14876 680 ** 14876 680 ** 14968 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 2686 680 ** 2686 680 ** 1944 680 ** 1944 680 ** 1944 680 ** 1944 680 ** 1944 680 ** 1944 680 ** 1944 680 ** 1944 680 ** 19536 680 ** 1954 680 ** 3596 680	svchost.exe executions. svchost.exe execution	38ab98be888 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 False Fa	3-12-26 18:38: 3-12-26 18:38: 18:37:52.00000 18:39:53.00000 18:39:53.00000 18:39:53.00000 18:39:53.00000 18:39:53.00000 18:41:23.00000 18:41:23.00000 18:41:23.00000 18:41:23.00000 18:41:23.00000 18:41:23.00000 18:41:24.00000 18:37:36.00000	49.000000 49.000000 N/A 00 N/A	N/A 3-12-26 N/A N/A N/A N/A N/A N/A N/A 000000 000000 000000	18:41:26.006 18:44:25.006 3-12-26 18: N/A N/A N/A N/A	999
** 1340 688 ** 14916 688 ** 14916 688 ** 14968 688 ** 1392 688 ** 1392 688 ** 1922 688 ** 1928 688 ** 1928 688 ** 1928 688 ** 1948 688 ** 2968 688 ** 2968 688 ** 2968 688 ** 1944 688 ** 1944 688 ** 1944 688 ** 1944 688 ** 1944 688 ** 1944 688 ** 1948 688 ** 1948 688 ** 1948 688 ** 3544 688 ** 3568 688 ** 1516 688 ** 3568 688 ** 1516 688 ** 3568 688 ** 1516 688 ** 3568 688 ** 1516 688 ** 3568 688 ** 1516 688 ** 3568 688 ** 1516 688 ** 3568 688 ** 1516 688 ** 3568 688 ** 1516 688 **	svchost.exe oxes svchos	38aby8be888 9 38aby8be888 5 38aby8be888 5 38aby8be888 5 38aby8be888 6 38aby8be888 6 38aby8be8988 6 38aby8be8988 6 38aby8be89888 6 38aby8be89888 6 38aby8be89888 6 38aby8be89888 6 38aby8be898888 6 38aby8be89888 6 38aby8be8988 6 38aby8be888 6 38aby8be8888 6 38aby8be888 6 38aby8be888 6 38aby8be8888 6		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 2023-12-26 2	3-12-26 18:38: 3-12-26 18:38: 18:37:52,00000 18:39:53,00000 18:39:53,00000 18:39:53,00000 18:39:53,00000 18:39:53,00000 18:39:53,00000 18:40:50,00000 18:40:50,000000 18:40:50,000000000000000000000000000000000	49.000000 49.000000 N/A 00 N/A	N/A 3-12-26 N/A N/A N/A N/A N/A N/A 000000 000000 000000 000000	18:41:26.006 18:44:25.006 18:44:25.006 3-12-26 18: N/A N/A N/A N/A N/A N/A	999
** 1340 688 ** 1416 688 ** 1416 688 ** 1417 688 ** 14187 688 ** 1490 688 ** 1490 688 ** 1490 688 ** 1292 688 ** 12	svchost.exe %xeisohost.exe %xeisohos	38aby8be888 9 9 1 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 2023-12-26 2	3-12-26 18:38: 3-12-26 18:38: 18:37:52, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:41-26 18:37:51, 00000 18:41-26 18:37:51, 00000 18:37:36, 00000	49.000000 49.000000 N/A 60 N/A	N/A 3-12-26 N/A N/A N/A N/A N/A N/A 000000 000000 000000 0000000 0000000 0000	18:41:26.006 18:44:25.006 3-12-26 18:: N/A N/A N/A N/A N/A	999
** 1340 680 ** 1476 680 ** 1476 680 ** 1476 680 ** 1968 680 ** 1992 680 ** 1992 680 ** 1992 680 ** 1928 680 ** 1928 680 ** 1928 680 ** 1948 680 ** 1948 680 ** 2988 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1948 680 ** 1964 680 ** 1964 680 ** 1964 680 ** 1964 680 ** 1964 680 ** 1968 680 ** 196	svchost.exe oxes svchost.exe svchost.exe oxes svchost.exe svchost.exe oxes svchost.exe svchost.exe oxes svch	38aby8be888 9 9 1 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	False	False 202 2023-12-26 2	3-12-26 18:38: 18:37:52, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:39:53, 00000 18:40, 00000 18:41, 000000 18:41, 000000 18:41, 000000 18:41, 000000 18:41, 000000 18:41, 000000 18:41, 000000 18:41, 000000 18:41, 000000 18:41, 000000000000000000000000000000000000	49.000000 49.000000 N/A 00 N/A	N/A 3-12-26 N/A N/A N/A N/A N/A N/A N/A N/A 000000 0000000 0000000 0000000	18:41:26.006 18:44:25.006 18:44:25.006 3-12-26 18: N/A N/A N/A N/A N/A N/A N/A	999

El tercer comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: "python vol.py -f C:\Herramientas\windows ram.mem windows.pstree.PsTree"

Este plugin se utiliza para visualizar la jerarquía de procesos en el sistema operativo Windows en forma de un árbol. Cada proceso se muestra como un nodo, y las relaciones de padre-hijo representan cómo se crearon los procesos.

Cuando se ejecuta este comando en un volcado de memoria de Windows, se obtiene una salida que muestra la relación jerárquica entre los procesos presentes en el sistema en el momento del volcado. Puede ser útil para entender cómo interactúan los diferentes procesos en el sistema.

2.4 Windows.privileges.Privs

```
Obligatility 3 7.4.0% underlity3-2.4.0 python vol.py -f C:\terramients\windows_ram.mem windows_privileges.Privs

Volatility 3 framework 2.4.0 pp Scanning finished progress; 100.00 process value Privilege Artibutes Description

System 2 SecretaFokomPrivilege Present Create a token object

System 3 SecsignPrisaryTokenPrivilege Present Create a token object

System 4 Second-privilege Present Replace a process-level token

System 5 Selncereas@outaPrivilege Present Increase quotabnity to desain

System 7 Selnchistings Present Replace quotas the dosain

System 8 SecondInjority great present frame quotast the dosain

System 9 SelakomershipPrivilege Present Increase quotabnity and security log system 9 SelakomershipPrivilege Present Ramage additing and security log system 9 SelakomershipPrivilege Present Increase quotabnity and security log system 9 SelakomershipPrivilege Present Increase volume for the system 12 SecondInjority privilege Present Increase quotabnity and security log system 9 SelakomershipPrivilege Present Change the system time.

System 10 SecondInjorityPrivilege Present Change the system time.

System 12 SecondInjorityPrivilege Present Change the system time.

System 13 SepretilesingleProcessPrivilege Present, Familed, Default Profile a single process

System 14 Selacomershipperivilege Present Change the system time.

System 15 Seconding Present Republication of the system time.

System 16 Seconding Privilege Present Change the system time.

System 17 Selacomerivilege Present Change the system time.

System 18 Selacomerivilege Present Republication of the system time.

System 19 Selacomerivilege Present Republication of the system system privilege Present Republication of the system system present greater than the system system present greater than the system present greater than the system present greater than th
```

El cuarto comando que hemos lanzado en volatility para analizar la memora ram que hemos extraído es el siguiente: "python vol.py -f C:\Herramientas\windows_ram.mem windows.privileges.Privs"

Este plugin se utiliza para listar los privilegios asignados a cada proceso en el sistema operativo Windows en el momento en que se creó el volcado de memoria.

Cuando ejecutas este comando, obtendrás una salida que muestra información sobre los procesos y los privilegios que tienen asignados. Los privilegios son derechos especiales que un proceso puede tener y que permiten realizar acciones específicas en el sistema.

Por ejemplo, la salida puede incluir información sobre procesos que tienen privilegios elevados, como el derecho a realizar acciones críticas en el sistema. Esto puede ser útil para la investigación de incidentes de seguridad y para comprender la configuración de seguridad del sistema en el momento del volcado de memoria.

En el pantallazo solo se muestra algunos pocos de la lista ya que el proceso era muy extenso.